

Detecting the quantum discord of an unknown state by a single observable

Chengjie Zhang^{1,*}, Sixia Yu^{1,2}, Qing Chen^{1,2}, and C.H. Oh^{1†}

¹*Department of Physics and Centre for Quantum Technologies,
National University of Singapore, 117542, Singapore*

²*Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics,
University of Science and Technology of China, Hefei, Anhui 230026, China*

We propose a single observable to witness the nonzero quantum discord of an unknown quantum state provided that we have four copies of the state. The expectation value of this observable provides a necessary and sufficient condition for nonzero quantum discord in $2 \times N$ systems and a necessary condition in higher finite-dimensional bipartite systems. Furthermore, a nontrivial lower bound of quantum discord can be obtained from this expectation value. The proposed observable can be experimentally measured in exactly the same easy manner as that of the entanglement witness, moreover a quantum circuit is designed to determine the expectation value of our observable with four simultaneous local qubit-measurements.

PACS numbers: 03.67.-a, 03.65.Ta, 03.67.Lx

I. INTRODUCTION

Entanglement is an essential resource in almost all quantum computing and informational processing tasks. In certain quantum computing tasks, however, there are still quantum advantages with the absence of entanglement. One typical example is the deterministic quantum computation with one qubit (DQC1) [1] in which the *quantum discord*, introduced by Ollivier and Zurek [2] and independently by Henderson and Vedral [3], is proposed to be responsible for the quantum speedup [4]. Ever since, the quantum discord, a nonnegative number quantifying all the quantum correlations in a state beyond the entanglement, has attracted much interest in quantum information theory [5–13]. Subsequently the operational meaning of the quantum discord has established firmly its status as an essential resource [14].

Quantum discord provides a measure for the quantum correlation beyond entanglement, which is defined as

$$D_A(\varrho) = \min_{\{E_k\}} \sum_k p_k S(\varrho_{B|k}) + S(\varrho_A) - S(\varrho), \quad (1)$$

where $S(\varrho) = -\text{Tr}(\varrho \log_2 \varrho)$ is the von Neumann entropy, ϱ_A (ϱ_B) is the reduced density matrix of subsystem A (B), and the minimum is taken over all possible positive operator-valued measures $\{E_k\}$ on subsystem A [3] with $p_k = \text{Tr}(E_k \otimes \mathbb{1}\varrho)$ and $\varrho_{B|k} = \text{Tr}_A(E_k \otimes \mathbb{1}\varrho)/p_k$. The minimum can also be taken over all the von Neumann measurements [2], and these two definitions coincide in the case of zero quantum discord. In general, the quantum discord is asymmetric, i.e., $D_A(\varrho)$ is not equal to $D_B(\varrho)$ which is obtained by measuring subsystem B . For simplicity we only consider $D_A(\varrho)$ in the following.

Though almost all quantum states have nonzero quantum discord [15], states with vanishing quantum discord

find numerous applications in fundamental concepts in addition to its initial motivation in pointer states [2]. For examples, the vanishing quantum discord is related to the complete positivity of a map [16] and the local broadcasting of the quantum correlations [17, 18]. For a given bipartite state in a finite-dimensional system, sufficient conditions as well as necessary and sufficient conditions for nonzero quantum discord have been proposed [19–22] in the form of local commutativity, strong positive partial transpose, etc. Specially Rahimi and SaiToh [23] have introduced an example of nonlinear witness for the nonzero quantum discord. All these criteria, however, require some knowledge of the quantum states and have nothing to say about the nonzero values of the quantum discord. The problem of witnessing the nonzero quantum discord of an unknown state remains open.

In this paper we shall propose a single observable to detect the nonzero quantum discord of a completely unknown state provided that we have four copies of the state. The expectation value of this observable provides not only a necessary and sufficient condition for nonzero quantum discord in $2 \times N$ systems and a necessary condition in higher finite-dimensional bipartite systems, but also quantitative lower bounds for the quantum discord and the geometric measure of quantum discord. Our observable can be experimentally measured in exactly the same easy manner as that of the entanglement witness, and moreover a quantum circuit is designed so that its expectation value can be easily determined via four simultaneous local qubit-measurements.

II. SINGLE-OBSERVABLE DETECTION OF QUANTUM DISCORD

It turns out that, similarly to entanglement witnesses, there is a Hermitian observable W that detects perfectly the nonzero quantum discord without state tomography and provides a lower bound for the quantum discord. To construct this observable we note firstly an important

*Electronic address: cqtzcj@nus.edu.sg

†Electronic address: phyohch@nus.edu.sg

lesson learned from [23] that a linear witness can never detect nonzero discord of a separable state. Therefore nonlinear witnesses should be used to detect quantum discord and the expectation values of an observable on multi copies of a state is naturally nonlinear. Secondly, since the quantum discord is invariant under local unitary (LU) transformations, the observable witnessing the quantum discord should also be LU-invariant.

In general, the polynomial LU invariants of degree k for a bipartite given quantum state ϱ_{AB} is given by $\text{Tr}(U\varrho^{\otimes k})$, where U is a tensor product of some permutation operator acting on copies of subsystem A and some permutation operator of subsystem B [24]. For later use we introduce the following four LU invariants $\text{Tr}(U_i\varrho^{\otimes 4})$ ($i = 1, 2, 3, 4$) of order 4 where

$$\begin{aligned} U_1 &= V_{14}^A V_{23}^A V_{12}^B V_{34}^B, & U_2 &= V_{14}^A V_{12}^B V_{34}^B, \\ U_3 &= V_{12}^A V_{34}^A V_{12}^B V_{34}^B, & U_4 &= V_{12}^A V_{12}^B V_{34}^B, \end{aligned} \quad (2)$$

in which we have denoted by $V_{ij}^{A,B} = \sum_{kl} |kl\rangle\langle lk|_{ij}^{A,B}$ the swapping operator acting on the i -th and the j -th copies of subsystem A (B). Our discord witness reads

$$W = U_1 - U_3 - \frac{2}{d_A}(U_2 - U_4), \quad (3)$$

where d_A is the dimension of \mathcal{H}_A and obviously $\text{Tr}(W\varrho^{\otimes 4})$ is also an LU-invariant. We are now ready to present our main result with the proof shown in the appendix:

Theorem. For an unknown bipartite state ϱ of a $d_A \times d_B$ system with 4 copies, if $\text{Tr}(W\varrho^{\otimes 4}) = 0$ then $D_A(\varrho) = 0$, conversely if $D_A(\varrho) = 0$ then $\text{Tr}(W\varrho^{\otimes 4}) = 0$ when $d_A = 2$. Moreover, if one restricts to von Neumann measurements in Eq. (1),

$$D_A(\varrho) \geq \max\{0, S(\varrho_A) - S(\varrho) - \log_2[d_A Q(\varrho)]\} \quad (4)$$

can be obtained, where

$$Q(\varrho) := \frac{\text{Tr}\varrho_B^2}{d_A} + (d_A - 1)\sqrt{\text{Tr}(W\varrho^{\otimes 4}) + (\text{Tr}\tilde{\varrho}^2)^2} \quad (5)$$

with $\tilde{\varrho} := \varrho - \mathbb{1}_A/d_A \otimes \varrho_B$.

Remark 1. The expectation value of W provides not only a necessary and sufficient condition for nonzero quantum discord in $2 \times N$ systems, but also a necessary condition in $M \times N$ systems with $M > 2$.

Remark 2. Similarly to Eq. (4), one can also present a nontrivial lower bound for the geometric measure of quantum discord using the expectation value of W , i.e.,

$$D_A^{(2)}(\varrho) \geq \max\{0, \text{Tr}\varrho^2 - Q(\varrho)\}. \quad (6)$$

$D_A^{(2)}(\varrho)$ is the geometric measure of quantum discord defined as [20]

$$D_A^{(2)}(\varrho) = \min_{\chi \in \Omega_0} \|\varrho - \chi\|^2, \quad (7)$$

where Ω_0 denotes the set of zero-discord states and $\|X - Y\|^2 = \text{Tr}[(X - Y)^2]$ is the square norm in the Hilbert-Schmidt space.

Remark 3. Suppose that $\{A_i\}_{i=0}^{d_A^2-1}$ and $\{B_j\}_{j=0}^{d_B^2-1}$ are complete sets of local orthogonal observables (LOOs) for subsystem A and B [25], respectively, which satisfy $\text{Tr}(A_i A_j) = \text{Tr}(B_i B_j) = \delta_{ij}$ with $A_0 = \mathbb{1}^A/\sqrt{d_A}$ and $B_0 = \mathbb{1}^B/\sqrt{d_B}$. Denote that $r_{ij} = \langle A_i \otimes B_j \rangle_\varrho$, and $R := (r_{ij})$ for $i = 1, \dots, d_A^2 - 1$ and $j = 0, \dots, d_B^2 - 1$ is a $(d_A^2 - 1) \times (d_B^2)$ dimensional matrix. Thus,

$$\varrho = \sum_{i=1}^{d_A^2-1} \sum_{j=0}^{d_B^2-1} r_{ij} A_i \otimes B_j + \frac{\mathbb{1}^A}{d_A} \otimes \varrho_B. \quad (8)$$

It can be obtained that $\text{Tr}(RR^T) = \sum_{i=1}^{d_A^2-1} \sum_{j=0}^{d_B^2-1} \langle A_i \otimes B_j \rangle_\varrho \langle A_i \otimes B_j \rangle_\varrho = \text{Tr}(\bar{V}_{12}^A V_{12}^B \varrho^{\otimes 2})$, where we have used $V^B = \sum_{j=0}^{d_B^2-1} B_j \otimes B_j$ and defined $\bar{V}^A := \sum_{i=1}^{d_A^2-1} A_i \otimes A_i = V^A - \mathbb{1}^A \otimes \mathbb{1}^A/d_A$. Similarly, we have $\text{Tr}[(RR^T)^2] = \sum_{i,k=1}^{d_A^2-1} \sum_{j,l=0}^{d_B^2-1} \langle A_i \otimes B_j \rangle_\varrho \langle A_k \otimes B_j \rangle_\varrho \langle A_k \otimes B_l \rangle_\varrho \langle A_i \otimes B_l \rangle_\varrho = \text{Tr}(\bar{V}_{14}^A \bar{V}_{23}^A V_{12}^B V_{34}^B \varrho^{\otimes 4})$. Therefore,

$$\text{Tr}[(RR^T)^2] - [\text{Tr}(RR^T)]^2 = \text{Tr}(W' \varrho^{\otimes 4}) = \text{Tr}(W \varrho^{\otimes 4}), \quad (9)$$

where $W' = \bar{V}_{14}^A \bar{V}_{23}^A V_{12}^B V_{34}^B - \bar{V}_{12}^A \bar{V}_{34}^A V_{12}^B V_{34}^B$ and the second equality holds since the invariance of $\varrho^{\otimes 4}$ under arbitrary permutation of different copies. From Eq. (9), one can see that W is related to the rank of R and the expectation value of W is always non-positive for arbitrary states.

Let us take the output state of DQC1 model as an example. The model of DQC1 introduced by Knill and Laflamme can evaluate the normalized trace of a unitary matrix efficiently [1]. Initially there is a single control qubit in the state $(\mathbb{1} + \alpha\sigma_z)/2$ with α describing the purity of the control qubit and a collection of n qubits in the completely mixed state $\mathbb{1}_n/2^n$. After the Hadamard gate applied to the control qubit and a control n -qubit unitary gate U_n , the output state becomes

$$\varrho_{out} = \frac{1}{2^{n+1}} \begin{pmatrix} \mathbb{1}_n & \alpha U_n^\dagger \\ \alpha U_n & \mathbb{1}_n \end{pmatrix}. \quad (10)$$

By making the measurements in the eigenbasis of σ_x and σ_y on the control qubit, the quantum circuit provides the normalized trace of U_n , $\tau = \text{Tr}(U_n)/2^n$, since the expectation values of σ_x and σ_y give estimates for the real and imaginary parts of τ , respectively.

There is strong evidence that DQC1 task cannot be simulated efficiently using classical computation [26], and the quantum discord has been proposed as a figure of merit for characterizing the resources present in this computational model [4]. It is worth noticing that the output state (10) is a natural $2 \times N$ state under the bipartite split between the control qubit and the collection of n qubits. Therefore, we can derive an explicit condition for characterizing the correlations in the output state using the

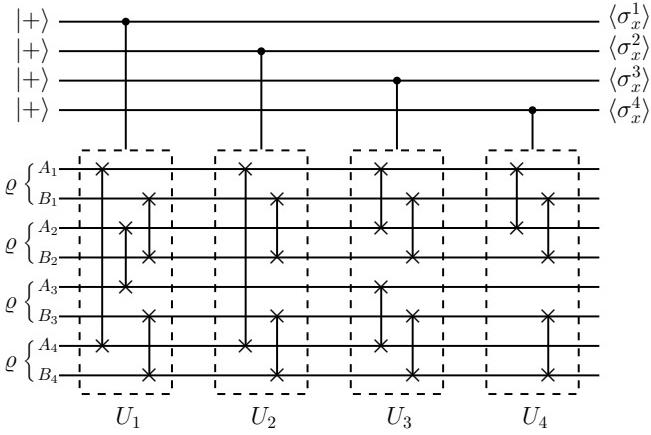


FIG. 1: Quantum circuit to measure the quantum discord witness W . Four auxiliary qubits, initially prepared in state $|+\rangle$, are control qubits for controlled- U_i ($i = 1, 2, 3, 4$) operations. Each U_i is composed of several controlled-swapping gates which are represented by connected crosses. After all the controlled- U_i operations, we perform σ_x -measurements on the auxiliary qubits and via Eq. (13) in the text value of $\text{Tr}(W\varrho^{\otimes 4})$ can be obtained.

theorem. After some algebra, we have

$$\text{Tr}(W\varrho_{out}^{\otimes 4}) = \frac{\alpha^4}{2^{2n+3}} \left(\left| \frac{\text{Tr}U_n^2}{2^n} \right|^2 - 1 \right). \quad (11)$$

According to our theorem, $D_A(\varrho_{out}) = 0$ if and only if $\text{Tr}(W\varrho_{out}^{\otimes 4}) = 0$, i.e., $\alpha = 0$ or $U_n^2 = e^{i\phi}\mathbb{1}_n$ for some real ϕ , which is equivalent to the result shown in Ref. [20].

On the other hand, if $\text{Tr}U_n = 0$ and $\alpha = 1$, using Eq. (4) we have a lower bound

$$D_A(\varrho_{out}) \geq 1 - \log_2 \left(1 + \sqrt{2^{2n+2}\text{Tr}(W\varrho_{out}^{\otimes 4}) + 1} \right), \quad (12)$$

for the quantum discord in DQC1. It is obvious that the negative expectation value $\text{Tr}(W\varrho_{out}^{\otimes 4})$ provides a non-trivial lower bound for $D_A(\varrho_{out})$. It has been shown that for almost every unitary matrix U_n (random unitary) the discord in the output state (10) is nonvanishing [4]. However, in the nontrivial case $U_n^2 = e^{i\phi}\mathbb{1}_n$ the quantum discord $D_A(\varrho_{out}) = 0$, which provides a counter example for the nonvanishing quantum discord of every nontrivial unitary matrix U_n . Thus, the quantum discord might not be the reason for the quantum speedup in DQC1.

III. MEASURING THE DISCORD WITNESS W

In order to measure the expectation value of the observable W we have designed a quantum circuit as shown in Fig. 1. We have introduced four auxiliary qubits, which are all initially prepared in the state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. After the controlled- U_i ($i =$

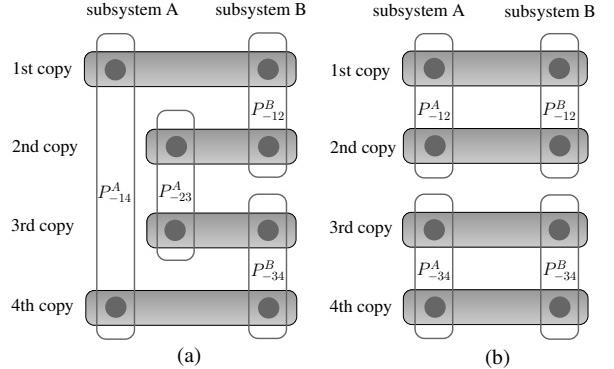


FIG. 2: Illustration of direct measurement of the observable W using four copies of ϱ . There are two measurement settings $P_{-14}^A P_{-23}^A P_{-12}^B P_{-34}^B$ and $P_{-12}^A P_{-34}^A P_{-12}^B P_{-34}^B$ corresponding to (a) U_1 and U_2 , and (b) U_3 and U_4 .

$1, \dots, 4$) operations with each qubit as source, we perform σ_x -measurements on all four auxiliary qubits so that four expectation values are obtained simultaneously. As it turns out $\langle \sigma_x^1 \rangle = \text{Tr}(U_1\varrho^{\otimes 4})$, $\langle \sigma_x^2 \rangle = \text{Tr}(U_2\varrho^{\otimes 4})$, $\langle \sigma_x^3 \rangle = \frac{1}{2}(\text{Tr}(U_3\varrho^{\otimes 4}) + \langle \sigma_x^1 \rangle)$, and $\langle \sigma_x^4 \rangle = \frac{1}{2}(\text{Tr}(U_4\varrho^{\otimes 4}) + \langle \sigma_x^2 \rangle)$, from which one can easily calculate the value of $\text{Tr}(W\varrho^{\otimes 4})$ according to

$$\text{Tr}(W\varrho^{\otimes 4}) = 2(\langle \sigma_x^1 \rangle - \langle \sigma_x^3 \rangle) - \frac{4}{d_A}(\langle \sigma_x^2 \rangle - \langle \sigma_x^4 \rangle). \quad (13)$$

Besides the quantum circuit shown above, one can also directly measure the single observable without the quantum circuit. Let $P_- = (\mathbb{1} - V)/2$ be the antisymmetric projector on some two copies and we have $V = \mathbb{1} - 2P_-$ so that we can expand W with P_{-ij} as what follows

$$\begin{aligned} W = & (\mathbb{1}_{14}^A - 2P_{-14}^A) \otimes \left(\frac{d_A - 2}{d_A} \mathbb{1}_{23}^A - 2P_{-23}^A \right) \\ & \otimes (\mathbb{1}_{12}^B - 2P_{-12}^B) \otimes (\mathbb{1}_{34}^B - 2P_{-34}^B) \\ & - (\mathbb{1}_{12}^A - 2P_{-12}^A) \otimes \left(\frac{d_A - 2}{d_A} \mathbb{1}_{34}^A - 2P_{-34}^A \right) \\ & \otimes (\mathbb{1}_{12}^B - 2P_{-12}^B) \otimes (\mathbb{1}_{34}^B - 2P_{-34}^B). \end{aligned} \quad (14)$$

Since the measurement of the observable $P_{-14}^A P_{-23}^A P_{-12}^B P_{-34}^B$ gives also information about observables like $P_{-23}^A P_{-12}^B P_{-34}^B$, etc., we need only two measurement settings $P_{-14}^A P_{-23}^A P_{-12}^B P_{-34}^B$ and $P_{-12}^A P_{-34}^A P_{-12}^B P_{-34}^B$ to measure the observable W . We illustrate these two measurement settings in Fig. 2(a) and Fig. 2(b), respectively.

For qubits, P_- takes the particularly simple form $P_- = |\psi^-\rangle\langle\psi^-|$ with $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$, and it has already been measured in several experiments using two copies of ϱ . For example, there are at least two methods to measure P_- in photonic system. The first method to project two photons onto the singlet state is to use a Hong-Ou-Mandel interferometer [27], which has been

used in [28]. The second method, employed in [29], is to distinguish the Bell states with a controlled-NOT gate, which can transform the Bell states to separable states.

Each of the two approaches proposed above to obtain the value of $\text{Tr}(W\rho^{\otimes 4})$, namely by the quantum circuit and the direct measurement, has its own advantages. The quantum circuit requires only one local measurement setting, but it needs the help of four auxiliary qubits and four controlled- U gates. The direct measurement of W does not require any auxiliary qubit, however, it needs two measurement settings. Compared with the quantum circuit, the direct measurement of W might be a little easier to realize in experiments, since the measurement of P_- for qubits has been realized in experiments.

IV. DISCUSSION AND CONCLUSION

In this work, we present a single observable W to witness the quantum discord of an unknown state provided there are four copies of the state. The expectation value of our observable provides a necessary condition for nonzero quantum discord which turns out to be also sufficient in $2 \times N$ systems. Also a nontrivial lower bound, which is illustrated in the example of DQC1, is placed by the discord witness. Moreover, a quantum circuit is designed to determine the expectation value of the discord witness W using four simultaneous local qubit-measurements. Interestingly, four copies of states have

also been turned out to be sufficient for entanglement detection of two-qubit states [30].

ACKNOWLEDGMENTS

This work is supported by National Research Foundation and Ministry of Education, Singapore (Grant No. WBS: R-710-000-008-271) and NNSF of China (Grant No. 11075227).

APPENDIX

We will present the calculation details to support our results and statements in the main text.

Complete proof of the Theorem. Suppose that $\{A_i\}_{i=0}^{d_A^2-1}$ and $\{B_j\}_{j=0}^{d_B^2-1}$ are complete sets of LOOs for subsystem A and B [25], respectively, which satisfy $\text{Tr}(A_i A_j) = \text{Tr}(B_i B_j) = \delta_{ij}$ with $A_0 = \mathbb{1}^A/\sqrt{d_A}$ and $B_0 = \mathbb{1}^B/\sqrt{d_B}$. As an example, one can choose $A_0 = \mathbb{1}^A/\sqrt{d_A}$, $B_0 = \mathbb{1}^B/\sqrt{d_B}$, $\{A_i\}_{i=1}^{d_A^2-1}$ and $\{B_j\}_{j=1}^{d_B^2-1}$ as the normalized traceless Hermitian generators of $SU(d_A)$ $\{\lambda_i\}_{i=1}^{d_A^2-1}$ and $SU(d_B)$ $\{\tilde{\lambda}_j\}_{j=1}^{d_B^2-1}$, respectively, i.e., $\text{Tr}\lambda_i = \text{Tr}\tilde{\lambda}_j = 0$ and $\text{Tr}(\lambda_i \lambda_j) = \text{Tr}(\tilde{\lambda}_i \tilde{\lambda}_j) = \delta_{ij}$. Therefore any bipartite density matrix has expansion

$$\rho = \frac{\mathbb{1}^A}{d_A} \otimes \frac{\mathbb{1}^B}{d_B} + \sum_{i=1}^{d_A^2-1} x_i \lambda_i \otimes \frac{\mathbb{1}^B}{\sqrt{d_B}} + \sum_{j=1}^{d_B^2-1} y_j \frac{\mathbb{1}^A}{\sqrt{d_A}} \otimes \tilde{\lambda}_j + \sum_{i=1}^{d_A^2-1} \sum_{j=1}^{d_B^2-1} t_{ij} \lambda_i \otimes \tilde{\lambda}_j, \quad (15)$$

where the coefficients x_i, y_j, t_{ij} forms the column vectors \mathbf{x}, \mathbf{y} and the $(d_A^2 - 1) \times (d_B^2 - 1)$ dimensional matrix T , respectively.

Denote by R a $(d_A^2 - 1) \times (d_B^2)$ dimensional matrix whose matrix elements are $r_{ij} = \langle A_i \otimes B_j \rangle_\rho$ with $i = 1, \dots, d_A^2 - 1$ and $j = 0, \dots, d_B^2 - 1$. For the state ρ given in Eq. (15), we have

$$R = (\mathbf{x}_{(d_A^2-1) \times 1} | T_{(d_A^2-1) \times (d_B^2-1)}). \quad (16)$$

In general we have

$$\begin{aligned} \rho &= \sum_{i=0}^{d_A^2-1} \sum_{j=0}^{d_B^2-1} r_{ij} A_i \otimes B_j \\ &= \sum_{i=1}^{d_A^2-1} \sum_{j=0}^{d_B^2-1} r_{ij} A_i \otimes B_j + \frac{\mathbb{1}^A}{d_A} \otimes \varrho_B, \end{aligned} \quad (17)$$

where $r_{0j} := \langle A_0 \otimes B_j \rangle_\rho$ and we have used

$$\begin{aligned} &\sum_{j=0}^{d_B^2-1} r_{0j} A_0 \otimes B_j \\ &= \sum_{j=0}^{d_B^2-1} r_{0j} \frac{\mathbb{1}^A}{\sqrt{d_A}} \otimes B_j \\ &= \sum_{j=0}^{d_B^2-1} \frac{1}{\sqrt{d_A}} \text{Tr}(\varrho_B B_j) \frac{\mathbb{1}^A}{\sqrt{d_A}} \otimes B_j \\ &= \frac{\mathbb{1}^A}{d_A} \otimes \varrho_B, \end{aligned} \quad (18)$$

since $r_{0j} = \langle \mathbb{1}^A/\sqrt{d_A} \otimes B_j \rangle_\rho = \text{Tr}(\varrho_B B_j)/\sqrt{d_A}$. A

straightforward calculation yields

$$\begin{aligned}
& \text{Tr}(RR^T) \\
&= \sum_{i=1}^{d_A^2-1} \sum_{j=0}^{d_B^2-1} r_{ij} r_{ij} \\
&= \sum_{i=1}^{d_A^2-1} \sum_{j=0}^{d_B^2-1} \langle A_i^1 \otimes B_j^1 \rangle_\varrho \langle A_i^2 \otimes B_j^2 \rangle_\varrho \\
&= \sum_{i=1}^{d_A^2-1} \sum_{j=0}^{d_B^2-1} \text{Tr}((A_i^1 \otimes B_j^1) \otimes (A_i^2 \otimes B_j^2)(\varrho^{\otimes 2})) \\
&= \text{Tr}(\bar{V}_{12}^A V_{12}^B \varrho^{\otimes 2}),
\end{aligned} \tag{19}$$

where A_i^m and B_j^n operate on the m th subsystem A and the n th subsystem B , respectively. We have used the swap operator

$$V_{12}^B = \sum_{j=0}^{d_B^2-1} B_j^1 \otimes B_j^2, \tag{20}$$

which operates on the first and second copies of subsystem B , and defined

$$\bar{V}_{12}^A := \sum_{i=1}^{d_A^2-1} A_i^1 \otimes A_i^2 = V_{12}^A - \frac{\mathbb{1}^A}{\sqrt{d_A}} \otimes \frac{\mathbb{1}^A}{\sqrt{d_A}}, \tag{21}$$

operating on the first and second copies of subsystem A . Notice that the swap operator is defined as

$$V := \sum_{kl} |k\rangle\langle l| \otimes |l\rangle\langle k|. \tag{22}$$

It is worth noticing that every Hermitian operator can be written in the operator basis, for example, the swap operator V_{12}^B on the first and second copies of subsystem B can be written as

$$V_{12}^B = \sum_{i,j=0}^{d_B^2-1} c_{ij} B_i^1 \otimes B_j^2, \tag{23}$$

where

$$\begin{aligned}
c_{ij} &= \text{Tr}(B_i^1 \otimes B_j^2 V_{12}^B) \\
&= \sum_{kl} \langle l | B_i^1 | k \rangle \langle k | B_j^2 | l \rangle \\
&= \text{Tr}(B_i^1 B_j^2) \\
&= \delta_{ij}.
\end{aligned} \tag{24}$$

Hence, one can directly obtain Eq. (20) using Eqs. (23) and (24). On the other hand, we have

$$\begin{aligned}
& \text{Tr}[(RR^T)^2] \\
&= \sum_{i,k=1}^{d_A^2-1} \sum_{j,l=0}^{d_B^2-1} \langle A_i^1 \otimes B_j^1 \rangle_\varrho \langle A_k^2 \otimes B_l^2 \rangle_\varrho \langle A_k^3 \otimes B_l^3 \rangle_\varrho \langle A_i^4 \otimes B_l^4 \rangle_\varrho \\
&= \text{Tr}(\bar{V}_{14}^A \bar{V}_{23}^A V_{12}^B V_{34}^B \varrho^{\otimes 4}).
\end{aligned} \tag{25}$$

Therefore,

$$\text{Tr}[(RR^T)^2] - [\text{Tr}(RR^T)]^2 = \text{Tr}(W' \varrho^{\otimes 4}) = \text{Tr}(W \varrho^{\otimes 4}) \tag{26}$$

where we have defined

$$W' := \bar{V}_{14}^A \bar{V}_{23}^A V_{12}^B V_{34}^B - \bar{V}_{12}^A \bar{V}_{34}^A V_{12}^B V_{34}^B, \tag{27}$$

and the second equality in Eq. (26) holds since

$$\text{Tr}(V_{14}^A V_{12}^B V_{34}^B \varrho^{\otimes 4}) = \text{Tr}(V_{23}^A V_{12}^B V_{34}^B \varrho^{\otimes 4}), \tag{28}$$

$$\text{Tr}(V_{12}^A V_{12}^B V_{34}^B \varrho^{\otimes 4}) = \text{Tr}(V_{34}^A V_{12}^B V_{34}^B \varrho^{\otimes 4}), \tag{29}$$

which comes from the invariance of $\varrho^{\otimes 4}$ under arbitrary permutation of different copies.

(i). If $\text{Tr}(W \varrho^{\otimes 4}) = 0$ then we have $\text{Tr}[(RR^T)^2] = [\text{Tr}(RR^T)]^2$, which means that the rank of the matrix R is 0 or 1.

(ia) If $\text{rank}(R) = 0$, then $R = 0$. From Eq. (17), we can obtain

$$\varrho = \frac{\mathbb{1}^A}{d_A} \otimes \varrho_B, \tag{30}$$

which obviously has zero quantum discord $D_A(\varrho) = 0$.

(ib) If $\text{rank}(R) = 1$, then there exist real numbers α_i and β_j such that $r_{ij} = \alpha_i \beta_j$ with $i = 1, \dots, d_A^2 - 1$ and $j = 0, \dots, d_B^2 - 1$. It follows from Eq. (17) that

$$\varrho = \sum_{i=1}^{d_A^2-1} \alpha_i A_i \otimes \sum_{j=0}^{d_B^2-1} \beta_j B_j + \frac{\mathbb{1}^A}{d_A} \otimes \varrho_B, \tag{31}$$

Using the eigenvectors $\{\Pi_k\}$ of $\sum_{i=1}^{d_A^2-1} \alpha_i A_i$ one can get $\sum_k (\Pi_k \otimes \mathbb{1}) \varrho (\Pi_k \otimes \mathbb{1}) = \varrho$, i.e., $D_A(\varrho) = 0$.

Therefore, if $\text{Tr}(W \varrho^{\otimes 4}) = 0$ then we have $D_A(\varrho) = 0$.

(ii). Conversely if $d_A = 2$ and $D_A(\varrho) = 0$ then there exists an orthonormal basis $\{|\psi_1\rangle, |\psi_2\rangle\}$ of subsystem A and two density matrices ϱ_k^B of subsystem B such that

$$\varrho = p|\psi_1\rangle\langle\psi_1| \otimes \varrho_1^B + (1-p)|\psi_2\rangle\langle\psi_2| \otimes \varrho_2^B, \tag{32}$$

with $0 \leq p \leq 1$. Using Eq. (32), it is straightforward to check that $\text{Tr}(W \varrho^{\otimes 4}) = 0$. Therefore, for a $2 \times N$ state ϱ , the discord $D_A(\varrho) = 0$ if and only if $\text{Tr}(W \varrho^{\otimes 4}) = 0$.

Moreover, if we perform a von Neumann measurement $\{\Pi_k\}_{k=1}^{d_A}$ on the subsystem A then we will obtain the outcome k with probability $p_k = \text{Tr}(\Pi_k \otimes \mathbb{1} \varrho)$ leaving the subsystem B in the state $\varrho_{B|k} = \varrho'_{B|k}/p_k$ where $\varrho'_{B|k} =$

$\text{Tr}_A(\Pi_k \otimes \mathbb{1}\varrho)$. The conditional entropy becomes

$$\begin{aligned}
& \sum_{k=1}^{d_A} p_k S(\varrho_{B|k}) \\
&= \sum_{k=1}^{d_A} p_k S(\varrho'_{B|k}/p_k) \\
&= - \sum_{k=1}^{d_A} \text{Tr}[\varrho'_{B|k} \log_2(\varrho'_{B|k}/p_k)] \\
&= \sum_{k=1}^{d_A} p_k \log_2 p_k - \sum_{k=1}^{d_A} \text{Tr}(\varrho'_{B|k} \log_2 \varrho'_{B|k}) \\
&= \sum_{k=1}^{d_A} p_k \log_2 p_k + S\left(\sum_{k=1}^{d_A} \Pi_k \otimes \varrho'_{B|k}\right) \\
&\geq -\log_2 d_A - \log_2 \left\{\sum_{k=1}^{d_A} \text{Tr}[(\varrho'_{B|k})^2]\right\}, \quad (33)
\end{aligned}$$

where we have used the inequalities $\sum_{k=1}^{d_A} p_k \log_2 p_k \geq -\log_2 d_A$ and $S(\varrho) \geq -\log_2 \text{Tr}\varrho^2$. By expanding Π_k using a complete set of LOOs with coefficients $e_i^k = \text{Tr}(\Pi_k A_i)$, i.e., $\Pi_k = \sum_{i=0}^{d_A-1} e_i^k A_i$, and denoting by M a $(d_A^2 - 1) \times (d_A^2 - 1)$ matrix with elements $M_{ij} = \text{Tr}(A_i^1 \otimes A_j^2 V_{12}^B \varrho^{\otimes 2})$, we obtain

$$\begin{aligned}
& \sum_{k=1}^{d_A} \text{Tr}[(\varrho'_{B|k})^2] \\
&= \sum_{k=1}^{d_A} \text{Tr}(V_{12}^B \varrho'_{B|k}) \\
&= \sum_{k=1}^{d_A} \sum_{i,j=0}^{d_A-1} e_i^k e_j^k \text{Tr}(A_i^1 \otimes A_j^2 V_{12}^B \varrho^{\otimes 2}) \\
&= \sum_{k=1}^{d_A} \sum_{i,j=1}^{d_A-1} e_i^k e_j^k M_{ij} + \frac{\text{Tr}\varrho_B^2}{d_A} \\
&\leq \sum_{k=1}^{d_A} \sum_{i=1}^{d_A-1} (e_i^k)^2 \sqrt{\text{Tr}(MM^T)} + \frac{\text{Tr}\varrho_B^2}{d_A} \\
&= (d_A - 1) \sqrt{\text{Tr}(W\varrho^{\otimes 4}) + (\text{Tr}\tilde{\varrho}^2)^2} + \frac{\text{Tr}\varrho_B^2}{d_A} \\
&:= Q(\varrho), \quad (34)
\end{aligned}$$

where we have used the Cauchy-Schwarz inequality, $\sum_{i=1}^{d_A-1} (e_i^k)^2 = (d_A - 1)/d_A$, and $\sum_{k=1}^{d_A} e_i^k = 0$ for $i = 1, \dots, d_A^2 - 1$. Therefore,

$$\begin{aligned}
& D_A(\varrho) \\
&= S(\varrho_A) - S(\varrho) + \min_{\{E_k\}} \sum_k p_k S(\varrho_{B|k}) \\
&\geq S(\varrho_A) - S(\varrho) - \log_2 d_A - \log_2 \left\{\sum_{k=1}^{d_A} \text{Tr}[(\varrho'_{B|k})^2]\right\} \\
&\geq S(\varrho_A) - S(\varrho) - \log_2 d_A - \log_2 [Q(\varrho)] \\
&= S(\varrho_A) - S(\varrho) - \log_2 [d_A Q(\varrho)], \quad (35)
\end{aligned}$$

which is the lower bound of the quantum discord Eq. (4) in the main text.

Remark. Similarly to Eq. (35), one can also present a nontrivial lower bound for the geometric measure of quantum discord $D_A^{(2)}(\varrho)$ using the expectation value of W , where $D_A^{(2)}(\varrho)$ is the geometric measure of quantum discord defined in Ref. [20]. Actually, Ref. [31] has shown that

$$D_A^{(2)}(\varrho) = \min_{\{\Pi_k\}} \left\{ \text{Tr}\varrho^2 - \sum_k \text{Tr}(\varrho'_{B|k})^2 \right\}, \quad (36)$$

Using Eq. (34), one can obtain

$$\begin{aligned}
D_A^{(2)}(\varrho) &= \min_{\{\Pi_k\}} \left\{ \text{Tr}\varrho^2 - \sum_k \text{Tr}(\varrho'_{B|k})^2 \right\} \\
&= \text{Tr}\varrho^2 - \max_{\{\Pi_k\}} \left\{ \sum_k \text{Tr}(\varrho'_{B|k})^2 \right\} \\
&\geq \text{Tr}\varrho^2 - Q(\varrho),
\end{aligned} \quad (37)$$

which is Eq. (6) in the main text.

DQC1 Model. The output state of DQC1 model can be written as

$$\begin{aligned}
\varrho_{out} &= \frac{1}{2^{n+1}} \begin{pmatrix} \mathbb{1}_n & \alpha U_n^\dagger \\ \alpha U_n & \mathbb{1}_n \end{pmatrix} \\
&= \frac{1}{2^{n+1}} (\mathbb{1}_1 \otimes \mathbb{1}_n + \alpha |1\rangle\langle 0| \otimes U_n + \alpha |0\rangle\langle 1| \otimes U_n^\dagger) \\
&= \frac{1}{2^{n+1}} \sum_{i,j=0}^1 \alpha^{(i+j)\text{mod}2} |i\rangle\langle j| \otimes U_n^i U_n^{\dagger j}.
\end{aligned} \quad (38)$$

Notice that for DQC1 model $d_A = 2$, thus

$$W = U_1 + U_4 - U_2 - U_3. \quad (39)$$

Based on Eq. (38), one can directly calculate as follows,

$$\begin{aligned}
\text{Tr}(U_1 \varrho_{out}^{\otimes 4}) &= \frac{1}{2^{4n+4}} (2^{2n+2} + 8\alpha^2 |\text{Tr}U_n|^2 \\
&\quad + 2\alpha^4 |\text{Tr}U_n^2|^2 + 2^{2n+1}\alpha^4),
\end{aligned} \quad (40)$$

$$\text{Tr}(U_2 \varrho_{out}^{\otimes 4}) = \frac{1}{2^{4n+4}} (2^{2n+3} + 8\alpha^2 |\text{Tr}U_n|^2), \quad (41)$$

$$\begin{aligned}
\text{Tr}(U_3 \varrho_{out}^{\otimes 4}) &= \frac{1}{2^{4n+4}} (2^{2n+2} + 2^{2n+3}\alpha^2 \\
&\quad + 2^{2n+2}\alpha^4),
\end{aligned} \quad (42)$$

$$\text{Tr}(U_4 \varrho_{out}^{\otimes 4}) = \frac{1}{2^{4n+4}} (2^{2n+3} + 2^{2n+3}\alpha^2). \quad (43)$$

Therefore,

$$\begin{aligned}
\text{Tr}(W \varrho_{out}^{\otimes 4}) &= \text{Tr}[(U_1 + U_4 - U_2 - U_3) \varrho_{out}^{\otimes 4}] \\
&= \frac{\alpha^4}{2^{2n+3}} \left(\left| \frac{\text{Tr}U_n^2}{2^n} \right|^2 - 1 \right),
\end{aligned} \quad (44)$$

which is Eq. (11) in the main text. According to our theorem, $D_A(\varrho_{out}) = 0$ if and only if $\text{Tr}(W \varrho_{out}^{\otimes 4}) = 0$, i.e., $\alpha = 0$ or $U_n^2 = e^{i\phi} \mathbb{1}_n$ for some real ϕ , which is equivalent to the result shown in Ref. [20]. It has been shown that

for almost every unitary matrix U_n (random unitary) the discord in the output state (38) is nonvanishing [4]. However, in the nontrivial case $U_n^2 = e^{i\phi} \mathbb{1}_n$ the quantum discord $D_A(\rho_{out}) = 0$, which provides a counter example for the nonvanishing quantum discord of every nontrivial unitary matrix U_n . Thus, the quantum discord might not be the reason for the quantum speedup in DQC1.

On the other hand, if $\text{Tr}U_n = 0$ and $\alpha = 1$, then for the output state Eq. (38) one can obtain that $\varrho_A = \mathbb{1}_1/2$, $\varrho_B = \mathbb{1}_n/2^n$, and the eigenvalues of ϱ_{out} are $\{0, \dots, 0, 1/2^n, \dots, 1/2^n\}$ in which there are 2^n copies of 0 and 2^n copies of $1/2^n$. Therefore,

$$S(\varrho_A) = 1, \quad (45)$$

$$S(\varrho_{out}) = n, \quad (46)$$

$$\text{Tr}\varrho_B^2 = \frac{1}{2^n}, \quad (47)$$

$$\text{Tr}\tilde{\varrho}_{out}^2 = \frac{1}{2^{n+1}}. \quad (48)$$

Using Eq. (35) we have a lower bound for the quantum discord in DQC1

$$D_A(\varrho_{out}) \geq 1 - \log_2 \left(1 + \sqrt{2^{2n+2} \text{Tr}(W\varrho_{out}^{\otimes 4}) + 1} \right), \quad (49)$$

which is Eq. (12) in the main text. It is obvious that the negative expectation value $\text{Tr}(W\varrho_{out}^{\otimes 4})$ provides a nontrivial lower bound for $D_A(\varrho_{out})$.

Measuring the discord witness W . In order to measure the expectation value of the observable W we have designed a quantum circuit as shown in Fig. 1 in the main text. We have introduced four auxiliary qubits, which are all initially prepared in the state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. After the controlled- U_i ($i = 1, \dots, 4$) operations with each qubit as source, we preform σ_x -measurements on all four auxiliary qubits so that four

expectation values are obtained simultaneously. As a result, the total state including the four auxiliary qubits is

$$\begin{aligned} \varrho_{total} = & \frac{1}{16} \sum_{i,i',\dots,l'} \left(|i\rangle\langle i'| \otimes |j\rangle\langle j'| \otimes |k\rangle\langle k'| \otimes |l\rangle\langle l'| \right. \\ & \left. \otimes U_4^l U_3^k U_2^j U_1^i \varrho_{out}^{\otimes 4} U_1^{\dagger i'} U_2^{\dagger j'} U_3^{\dagger k'} U_4^{\dagger l'} \right). \end{aligned} \quad (50)$$

Thus, we have

$$\begin{aligned} \langle \sigma_x^1 \rangle &= \frac{1}{2} [\text{Tr}(\varrho^{\otimes 4} U_1^\dagger) + \text{Tr}(U_1 \varrho^{\otimes 4})] \\ &= \text{Tr}(U_1 \varrho^{\otimes 4}), \end{aligned} \quad (51)$$

$$\begin{aligned} \langle \sigma_x^2 \rangle &= \frac{1}{2} [\text{Tr}(\varrho^{\otimes 4} U_2^\dagger) + \text{Tr}(U_2 \varrho^{\otimes 4})] \\ &= \text{Tr}(U_2 \varrho^{\otimes 4}), \end{aligned} \quad (52)$$

$$\begin{aligned} \langle \sigma_x^3 \rangle &= \frac{1}{4} [\text{Tr}(\varrho^{\otimes 4} U_3^\dagger) + \text{Tr}(U_3 \varrho^{\otimes 4}) + 2\langle \sigma_x^1 \rangle] \\ &= \frac{1}{2} [\text{Tr}(U_3 \varrho^{\otimes 4}) + \langle \sigma_x^1 \rangle], \end{aligned} \quad (53)$$

$$\begin{aligned} \langle \sigma_x^4 \rangle &= \frac{1}{4} [\text{Tr}(\varrho^{\otimes 4} U_4^\dagger) + \text{Tr}(U_4 \varrho^{\otimes 4}) + 2\langle \sigma_x^2 \rangle] \\ &= \frac{1}{2} [\text{Tr}(U_4 \varrho^{\otimes 4}) + \langle \sigma_x^2 \rangle], \end{aligned} \quad (54)$$

from which one can easily calculate the value of $\text{Tr}(W\varrho^{\otimes 4})$ according to

$$\text{Tr}(W\varrho^{\otimes 4}) = 2\left(\langle \sigma_x^1 \rangle - \langle \sigma_x^3 \rangle\right) - \frac{4}{d_A}\left(\langle \sigma_x^2 \rangle - \langle \sigma_x^4 \rangle\right), \quad (55)$$

which is Eq.(13) in the main text. In order to obtain Eq. (14) in the main text, one can use the definition of W Eqs. (2) and (3) in the main text and the equation $V = \mathbb{1} - 2P_-$.

- [1] E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998).
- [2] H. Ollivier and W. H. Zurek, Phys. Rev. Lett. **88**, 017901 (2001).
- [3] L. Henderson and V. Vedral, J. Phys. A **34**, 6899 (2001).
- [4] A. Datta, A. Shaji, and C. M. Caves, Phys. Rev. Lett. **100**, 050502 (2008).
- [5] K. Modi *et al.*, Phys. Rev. Lett. **104**, 080501 (2010).
- [6] M. D. Lang and C. M. Caves, Phys. Rev. Lett. **105**, 150501 (2010).
- [7] T. Werlang, C. Trippe, G. A. P. Ribeiro, and G. Rigolin, Phys. Rev. Lett. **105**, 095702 (2010).
- [8] P. Giorda and M. G. A. Paris, Phys. Rev. Lett. **105**, 020503 (2010); G. Adesso and A. Datta, *ibid.* **105**, 030501 (2010).
- [9] T. Werlang, S. Souza, F. F. Fanchini, and C. J. Villas Boas, Phys. Rev. A **80**, 024103 (2009).
- [10] J. Maziero, L. C. Céleri, R. M. Serra, and V. Vedral, Phys. Rev. A **80**, 044102 (2009).
- [11] F. F. Fanchini *et al.*, Phys. Rev. A **81**, 052107 (2010).
- [12] J. Maziero *et al.*, Phys. Rev. A **81**, 022116 (2010).
- [13] J.-S. Xu *et al.*, Nat. Commun. **1**, 7 (2010); J.-S. Xu *et al.*, Phys. Rev. A **82**, 042328 (2010).
- [14] D. Cavalcanti *et al.* Phys. Rev. A **83**, 032324 (2011); V. Madhok and A. Datta, Phys. Rev. A **83**, 032323 (2011).
- [15] A. Ferraro *et al.*, Phys. Rev. A **81**, 052318 (2010).
- [16] A. Shabani and D. A. Lidar, Phys. Rev. Lett. **102**, 100402 (2009); A. Shabani and D. A. Lidar, Phys. Rev. A **80**, 012309 (2009); C. A. Rodríguez-Rosario *et al.*, J. Phys. A **41**, 205301 (2008).
- [17] M. Piani, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **100**, 090502 (2008).
- [18] S. Luo and W. Sun, Phys. Rev. A **82**, 012338 (2010).
- [19] B. Bylicka, and D. Chruściński, Phys. Rev. A **81**, 062102 (2010).
- [20] B. Dakić, V. Vedral, and Č. Brukner, Phys. Rev. Lett. **105**, 190502 (2010).
- [21] A. Datta, arXiv:1003.5256.

- [22] L. Chen, E. Chitambar, K. Modi, and G. Vacanti, Phys. Rev. A **83**, 020101(R) (2011).
- [23] R. Rahimi, and A. SaiToh, Phys. Rev. A **82**, 022314 (2010).
- [24] M. Grassl, M. Rötteler, and T. Beth, Phys. Rev. A **58**, 1833 (1998); M. S. Leifer, N. Linden, and A. Winter, *ibid.* **69**, 052304 (2004); R. Brauer, Ann. Math. **38**, 857 (1937).
- [25] S. Yu and N.-L. Liu, Phys. Rev. Lett. **95**, 150504 (2005).
- [26] A. Datta and G. Vidal, Phys. Rev. A **75**, 042310 (2007).
- [27] C.-K. Hong, Z.-Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).
- [28] Y.-F. Huang *et al.*, Phys. Rev. A **79**, 052338 (2009).
- [29] S. P. Walborn *et al.*, Nature (London) **440**, 1022 (2006); S. P. Walborn *et al.*, Phys. Rev. A **75**, 032338 (2007); C. Schmid, *et al.*, Phys. Rev. Lett. **101**, 260505 (2008).
- [30] R. Augusiak, M. Demianowicz, and P. Horodecki, Phys. Rev. A **77**, 030301(R) (2008).
- [31] S. Luo and S. Fu, Phys. Rev. A **82**, 034302 (2010).